REMARKS/ARGUMENTS

Favorable consideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 1-20 are pending in the application, with Claim 3 amended by the present amendment.

In the outstanding Office Action, Claims 1-20 were rejected under 35 U.S.C. § 102(e) as being anticipated by Clark (U.S. Patent No. 5,982,897).

Claim 3 is amended to place the application in condition for appeal. No new matter is added.

Briefly recapitulating, Claim 1 is directed to a method for satellite positioning using positioning signals which are sent out by the various satellites of a satellite constellation under the control of a set of ground stations from which said satellites receive control signals. The position signals are available to be picked up by individual user receivers. The method includes (a1) emitting, from the set of ground stations, periodically renewed direct transformation functions which are addressed respectively to each satellite of said satellite constellation and (a2) applying the direct transformation function received by each satellite to encode the positioning signals emitted therefrom. The method further includes, (b1) upon each request from a user receiver addressed to a user servicing station, verifying that the user receiver has a right to a privileged-user status and, (b2) in the event that the verification is positive, addressing to the user receiver reverse transformation functions that are inverse to the direct transformation functions applied at the satellites from which it receives positioning signals. The reverse transformation functions constitute an interpretation key for interpreting the positioning signals by applying the reverse transformation functions for decoding them.

Clark describes a system and method for GPS key distribution and use.[1] In particular, Clark describes discloses a method and system wherein satellites that are visible from a hostile area do not transmit a decryption key for a high-precision navigational data, while satellites that are only visible from non-hostile areas do.[2] Hence, all the users situated in a "non-hostile" area benefit from an unrestricted access to high-precision navigational data.

However, contrary to the Official Action, Clark does not disclose or suggest Applicants' claimed feature of "(b1) upon each request from a user receiver addressed to a user servicing station, verifying that the user receiver has a right to a privileged-user status and, (b2) in the event that the verification is positive, addressing to the user receiver reverse transformation functions that are inverse to the direct transformation functions applied at the satellites from which it receives positioning signals." The reverse transformation functions constitute an interpretation key for interpreting the positioning signals by applying the reverse transformation functions for decoding them. In detail, Clark fails to disclose or suggest each of the following elements of Applicants' independent claim:

- a user receiver addressing a request to a user servicing station,

- the user servicing station verifying the user receiver has a privileged-user status; and

- in the event that the verification is positive, the user servicing station addressing to the user an interpretation key for interpreting positioning signals.

In Clark there is no request-and-identification procedure, nor selective transmission of an interpretation key to privileged users which have required it and have been identified as such: a decryption key is simply broadcast to all users situated in a "non-hostile" geographic area. Indeed, at column 6, lines 44 to 63, Clark discloses an embodiment wherein satellites broadcast an encoded decryption key. Authorized users receive a registration key, which allows them to decode the broadcast decryption key, and then use the latter to decode the

[1] Clark, abstract.
[2] Clark, column 4, lines 33 – 65.

high-precision navigational data. Nonetheless, this embodiment does not disclose a method wherein an interpretation or decryption key is selectively transmitted to users which have requested it and have been identified as "privileged".

It is important to underline a key difference between Clark and the present invention: In Clark, the satellites themselves broadcast a decryption key, independently from any request from users. The decryption key is itself encoded, and only registered users can decode it, due to their registration key. Assuming *arguendo* that there is a "user servicing station" in Clark, this would have to be the registration authority, which does not transmit a decryption or interpretation key, but only transmits a registration key which allows decoding the broadcast decryption key. In contrast, in the present invention, users actively request the specific delivery of the actual interpretation key (preferably, but not necessarily, in a coded form) from a user servicing station, which has full power to refuse the delivery if the user has not a "privileged" status or has lost it by behaving in an irregular way.

By way of further example and explanation, in Clark's system and method, the period of use of the registration key needs to have a much longer period of use than the encryption key (col. 6, lines 44 to 46). Therefore, once the registration key has been distributed, the system manager has no possibility of preventing the registered user of acceding to the high-precision navigational data, even if it begins acting in an unauthorized way.

For example, if the user is a civil airplane which receives, before taking-off, a registration key which is valid during all the scheduled flight time, if the airplane exits the authorized flight path, it will still benefit from the high-precision navigational data and the only way to prevent that would be to perform an unscheduled change of the code used for encoding the decryption key. This would affect all the registered users, by making their registration keys useless.

On the contrary, in Applicants' claimed system and method, the user has to ask for the interpretation key(s) each time he needs to access to the high-precision positioning service (it cannot rely on a previously obtained interpretation key, because the encryption key could have changed since then). At each request, the identity and behavior of the user can be checked, and it can be easily declared non-privileged if not complying with the system security requirements.

Another distinction and drawback of Clark's system and method is that, in "hostile" zones, even trustworthy civilian users, such as airplanes performing regular service, are denied access to the high-precision positioning service unless they have a military-type receiver incorporating the key generation function used in GPS satellites (see Clark, column 8, lines 37 - 43), which is highly unlikely. On the contrary, the system and method of the invention allows providing privileged civilian user with a controlled access to the high-precision positioning service for a specific mission only.

No passage in Clark either discloses or suggests a system and method wherein an interpretation key ("reverse transformation functions") is selectively transmitted upon request, to privileged users only, by a user servicing station. Thus, again Applicants submit Claims 1, 15 and 19 are not anticipated by and are not obvious in view of Clark

All the other claims depend from Claim 1, 15 or 19, and for this reason they are also new and non-obvious. Moreover, the specific limitations of many of these dependent claims are also new and non-obvious per se. Examples relative to Claims 2, 8, 9, 10, 13 and 14 follow:

As already discussed, Clark does not disclose nor suggest a method wherein requests are sent by users calling for an interpretation key. A fortiori, Clark does not disclose or suggest transmitting, together with such a request, a copy of the latest coded positioning signal the user receiver has picked up from the satellites (or more generally, of positioning

signals emitted from a plurality of satellites and received by the user receiver). Therefore Claims 2, 8, 9, 10, 13 and 14, all other claims reciting the above technical feature (with a slightly different wording for different claims) are new and non-obvious in view of Clark

Applicants further note that, in the Official Action issued on June 1st, 2005, the Examiner merely restated the rejection of Claims 2, 8, 9, 10, 13 and 14 a of November 16, 2004 without providing any response to the arguments filed by the Applicant on March 9, 2005. Applicants request consideration and a specific response to Applicants' previously presented arguments. These and other arguments are re-presented below:

As per Claim 2, at column 3, line 50 to column 4, line 10, Clark discloses a method wherein all the satellites transmit encrypted data and a decryption key, which is accessible to all users, which transmit neither a request, nor positional data. In the above-cited passage there is no disclosure of a transmission, from a user receiver to a user servicing station, of a copy of the latest coded positioning signal said user receiver has picked up from the satellites.

As per Claims 8 and 9, at column 7, lines 1 to 33 and at column 7, line 50 to column 8, line 5, Clark disclose a method an apparatus wherein a decryption key is broadcast in encoded form and wherein all registered users can autonomously decode said decryption key and use it to accede to high-precision navigational data. Again, there is no disclosure of a transmission, from a user receiver to a user servicing station, of a copy of the latest positioning signal received by said receiver, in their transformed form.

As per Claim 10, at column 5, lines 16 to 26 Clark discusses a drawback of his invention, namely the fact that even users outside an "hostile" area can suffer from an intermittent denial to accede to high-precision navigational data. Again, there is no disclosure of a transmission, from a user receiver to a user servicing station, of a copy of the latest coded positioning signal received by said receiver.

As per Claim 13, at column 5, lines 45 - 56 Clark discloses the use of a beam-steering technique, and at column 6, lines 28 - 53 Clark discloses the possibility of providing privileged users with the master key used for generating the encryption key, so that privileged users benefit from an unlimited access to high-precision navigational data. Again, there is no disclosure of a transmission, from a user receiver to a user servicing station, of a copy of the positioning signals emitted from a plurality of satellites as received by said user receiver (i.e. in coded or transformed form).

As per Claim 14, at column 4, lines 11 - 20 Clark discloses a periodical broadcasting of the decryption key to all users outside a "hostile" area. Again, there is no disclosure of a transmission, from a user receiver to a user servicing station, of a copy of the positioning signals emitted from a plurality of satellites as received by said user receiver (i.e. in coded or transformed form).

Regarding Claim 3, Clark does not disclose nor suggest supplying an identifier to the user and broadcasting it to various servicing stations to which the user is likely to address a request calling for an interpretation key. The rejection of Claim 3 appears to be that the Examiner considers that a ground based transmitter used to broadcast signals is the same thing as an identifier which is broadcast to various user servicing stations. (The actual basis of rejection is not clear from the Official Action). Assuming this hypothetical grounds of rejection is being relied upon, Applicants traverse this assumption. As customary in the field of telecommunications and as explicitly stated at page 18, line 34 - page 19, line 1 of the application, an "identifier" is a code which designates the user for the radio communications or a call signal: therefore a "ground based transmitter", i.e. a piece of hardware, cannot be an "identifier" in the sense in which this word is used in the present application. Moreover, Claim 3 states that "said identifier is broadcast to various user station". Clearly, a "ground based transmitter" cannot "be broadcast"; instead it is used to broadcast signals. As a

consequence, the passages cited by the Examiner (Clark, column 5, lines 36 - 44 and column 6, lines 44 to 52) have no relationship with Claim 3, which is therefore new and non-obvious in view of Clark. However, for the sake of clarity and in anticipation of appeal, Claim 3 is amended to explicitly state that the "identifier" is an identifier code which designate the user for a declared mission.

Regarding Claim 5, Applicant respectfully observes that, in the Official Action issued on June 1st, 2005 merely repeats the rejection of Claim 5 of November 16, 2004 without providing any response to the arguments filed by the applicant on March 9, 2005. This rejection is unjustified. Clark does not disclose nor suggest any authentication procedure, i.e. any verification of the authenticity or of the integrity of the code received by the user receiver (see page 32, lines 1 to 21 of the application). The passage cited by the Examiner (column 6, lines 33 to 39 of Clark) deals with a fully unrelated feature, namely the use of clock timing acquired from the satellites to generate a periodic key. Therefore Claim 5 is and non-obvious in view of Clark.

Regarding Claim 6, Clark does not disclose nor suggest any preliminary stage of invoicing the user benefiting from the privileged-user status. Rather, at column 6, lines 39 to 43, Clark mention the possibility of providing privileged users with the master key used for generating the encryption key, so that privileged users benefit from an unlimited access to high-precision navigational data. Therefore Claim 6 is new and non-obvious in view of Clark.

Regarding Claim 7, Applicants respectfully observe that in the Official Action issued on June 1st, 2005, the rejection of Claim 7 of November 16, 2004 is repeated without providing any response to the arguments filed by the Applicant on March 9 2005. This rejection is unjustified. Clark does not disclose nor suggest performing a comparison, carried out by a privileged-user receiver, between signals received from the satellites and signals

received from a service station processing a request for an interpretation key. The passages cited in the earlier Official Action (Clark, column 5, lines 57 to 43 and column 6, lines 28 to 43) deal with fully unrelated features, namely the possibility of providing privileged users with the master key used for generating the encryption key, so that privileged users benefit from an unlimited access to high-precision navigational data. Therefore Claim 7 is new and non-obvious in view of Clark.

Regarding Claim 11, Applicant respectfully observes that, in the Official Action issued on June 1st, 2005, the rejection of Claim 11 of November 16, 2004 is repeated without providing any response to the arguments filed by the applicant on March 9. 2005. This rejection is unjustified. Clark does not disclose nor suggest the use of a "basic" and a "supplementary" interpretation key; giving access to a different level of precision of navigational data. On the contrary, the cited passage at column 4, lines 45 - 65 makes clear that, according to Clark, users either receive the "full" decryption key or not, but there are no "basic" and "supplementary" keys. Therefore Claim 11 is new and non-obvious in view of Clark.

Regarding Claim 12, Applicants respectfully observe that, in the Official Action issued on June 1st, 2005, the rejection of Claim 12 of November 16, 2004 is merely repeated without providing any response to the arguments filed by the applicant on March 9, 2005. This rejection is unjustified. Clark does not disclose nor suggest a method wherein each transformation function participating in the definition of a decryption key is announced to the user servicing stations with an advance in time with respect to its application to the positioning signals sent out by the corresponding satellite. At column 7, line 50 to column 8, line 30 Clark simply suggests that the users acquire the decryption key even when the navigational data are not encrypted, in prevision of the possibility that the encryption mode will soon begin. Therefore Claim 12 is new and non-obvious in view of Clark.

Regarding Claim 18, Applicant respectfully observes that in the Official Action issued on June 1st, 2005, the rejection of Claim 18 of November 16, 2004 is merely repeated without providing any response to the arguments filed by the applicant on March 9. 2005. This rejection is unjustified. Clark does not disclose user servicing stations which receive the decryption key from a master station and transmit it to the users on request and subject to verification of their privileged status. On the contrary, at the passage cited by the Examiner (column 4, lines 33 to 65) Clark discloses a system in which a decryption key is continuously broadcast by all satellites which are not visible from a "hostile region", i.e. decryption key is transmitted to all users - privileged and not privileged - without the need for any request. Therefore Claim 12 is new and non-obvious in view of Clark

Regarding Claim 20, Applicant respectfully observes that in the Official Action issued on June 1st, 2005, the rejection of Claim 20 of November 16, 2004 is merely repeated without providing any response to the arguments filed by the applicant on March 9, 2005. This rejection is unjustified. As already discussed, in Clark there is no request from the users, therefore there is no request signal whose emission is automatically repeated by a user receiver. At column 8, lines 9 - 43 Clark discloses a system wherein transmission of a decryption key, together with positioning data, is periodically repeated by satellites. Therefore Claim 20 is new and non-obvious in view of Clark.

MPEP § 2131 notes that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "When a claim covers several structures or compositions, either generically or as alternatives, the claim is deemed anticipated if any of the structures or compositions within the scope of the claim is known in the prior art." *Brown v. 3M*, 265 F.3d 1349, 1351, 60 USPQ2d 1375, 1376 (Fed. Cir. 2001) (claim to a system for setting a

computer clock to an offset time to address the Year 2000 (Y2K) problem, applicable to records with year date data in "at least one of two-digit, three-digit, or four-digit" representations, was held anticipated by a system that offsets year dates in only two-digit formats). See also MPEP § 2131.02. "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Because Clark does not disclose or suggest all the features recited in Claims 1, 15 and 19, Clark does not anticipate the invention recited in Claims 1, 15 and 19, and all claims depending therefrom.

Accordingly, in view of the present amendment and in light of the previous discussion, Applicants respectfully submit that the present application is in condition for allowance and respectfully request an early and favorable action to that effect.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599

Michael E. Monaco
Registration No. 52,041

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\MM\AMENDMENT\369\208536.AM DUE 9-1-05.DOC